Configuring RME with Cisco Secure ACS

This section describes how RME is configured with Cisco Secure ACS:

- CiscoWorks Login Module
- CiscoWorks Server Authentication Roles
- Integration Notes
- Configuring RME on Cisco Secure ACS
- Verifying the RME and the Cisco Secure ACS Configuration

CiscoWorks Login Module

The CiscoWorks Server provides the mechanism used to authenticate users for CiscoWorks applications. CiscoWorks Common Services supports two modes of user authentication and authorization:

- ACS—In this mode authentication and authorization services are provided by an Access Control Server. To use this mode, you must have a Cisco Secure ACS (Access Control Server) installed on your network.

  The supported Cisco Secure ACS for Windows are:

  - Cisco Secure ACS 3.2
  - Cisco Secure ACS 3.2.3
  - Cisco Secure ACS 3.3.2

- Non ACS—In this mode authentication and authorization services are provided by CiscoWorks Server.

Fallback option in ACS mode is different from non-ACS mode. Here, fallback is provided only for authentication.

- If the user authentication with ACS fails, the authentication is tried with CiscoWorks local mode.
- If it succeeds, the user is allowed to change the login module to non-ACS mode, provided the user has permission to do that operation in non-ACS mode.

See User Guide for CiscoWorks Common Services 3.0 and CiscoWorks Common Services 3.0 Online Help for further details.

CiscoWorks Server Authentication Roles

By default, the CiscoWorks server authentication provides five roles in the ACS mode. They are listed here from least privileged to most privileged:

1. Help Desk—User with this role has the privileges to access network status information from the persisted data. User does not have the privilege to contact any device or schedule a job that will reach the network.

   For example: Inventory data, configuration archives, reports, Syslog messages, jobs status, etc.

2. Approver—User with this role has the privileges to approve all RME tasks.
3. Network Operator—User with this role has the privileges to perform all tasks that involve collecting data from the network. User does not have write access on the network. User can also perform all the Help Desk tasks.

   For example: Scheduling jobs for inventory, configuration collection, etc.

4. Network Administrator—User with this role has the privilege to change the network. User can also perform the Network Operator tasks.

   For example: Software Management tasks such as image distribution, NetConfig tasks such as changing the device passwords, configuration downloads etc.

5. System Administrator—User with this role has privilege to perform all CiscoWorks system administration tasks. See Permissions Report on CiscoWorks server (Common Services > Server > Reports > Permission Report).

   For example: Changing the RME Administration setting, defining the purge policy, etc.

We recommended that you do not modify the default CiscoWorks roles.

You can create your own custom roles on Cisco Secure ACS.

See User Guide for CiscoWorks Common Services 3.0 and CiscoWorks Common Services 3.0 Online Help for further details.

Integration Notes

This section contains notes that you should read before you begin Cisco Secure ACS and CiscoWorks server integration:

- We recommend that you integrate CiscoWorks server and Cisco Secure ACS after installing all LAN Management Solution applications.
- For RME, you must ensure that the CiscoWorks server System Identity Setup user has the privilege to perform all RME tasks on Cisco Secure ACS.
- If you have installed your application after configuring the CiscoWorks Login Module to ACS mode then the application users are not granted any permission.

  However, the application is registered to the Cisco Secure ACS. On the Cisco Secure ACS server, you must assign the appropriate permissions to the application.

  See Configuring RME server with Cisco Secure ACS.
- Multiple instances of same application using same Cisco Secure ACS will share settings. Any changes will affect all instances of that application.
- If application is configured with Cisco Secure ACS and then application is reinstalled, the application will inherit the old settings.

  This is applicable if you are using Cisco Secure ACS version 3.2.3.

- The role which you create is not shared across all the LAN Management Solution applications. The role which you create is shared across all CiscoWorks server that is configured to that particular Cisco Secure ACS.

  You have to create new roles for each of the LAN Management Solution applications that are running on the CiscoWorks server.

  For example, if you have configured 10 CiscoWorks servers with an Cisco Secure ACS. You have created a role in RME (say, “RMESU”). This role is shared for RME application that is running in all 10 CiscoWorks server.

  This role is not shared for any other LAN Management Solution applications that is running on the CiscoWorks server.

- You can have different users having different access privileges to the CiscoWorks applications.

  For example, if you have a user CWSU, this user can be System Administrator in Common Services, Approver in RME, Network Operator for Campus, Network Administrator for DFM, and Help Desk for IPM.

- Review User Guide for Common Services, Configuring the Server chapter for details on configuring the CiscoWorks Server in ACS mode.

Configuring RME on Cisco Secure ACS

After registering the CiscoWorks Server with Cisco Secure ACS perform the following on Cisco Secure ACS:

Step 1 Click **Shared Profile Components** to view the Resource Manager Essentials application entry is present.

Step 2 Based on your authentication setting (per user or per group) on Cisco Secure ACS, click either User Setup or Group Setup.

Step 3 On Cisco Secure ACS, you can verify the per user or per group setting for Resource Manager Essentials using Interface **Configuration > TACACS + (Cisco IOS)**.

Step 4 Assign the appropriate privileges to the User/Group to use the Resource Manager Essentials.

For RME, you must ensure that the CiscoWorks server System Identity Setup user has the privilege to perform all RME tasks on Cisco Secure ACS.

Verifying the RME and the Cisco Secure ACS Configuration

After performing the above mentioned tasks on Cisco Secure ACS server,

1. Login to CiscoWorks with the username as defined in the Cisco Secure ACS.
2. Based on your privilege on the Cisco Secure ACS, you can perform only certain tasks on the CiscoWorks server.

   For example: If your privilege is of Help Desk, then you can only View the Device Summary.
3. Based on the Network Device setting for the User/Group on the Cisco Secure ACS, you can view only certain devices in the CiscoWorks server.